10/069676, 020102

JC05 Rec'd PCT/PTO 21 FEB 2002

EXPRESS MAIL NO. EV064839849US

FORM PTO-1390 (REV 11-2000) DEPARTMENT OF COMMERCE PATENT AND TRADEMARK OFFICE		ATTORNEY'S DOCKET NO
TRANSMITTAL LETTER TO THE UNITED STATES DESIGNATED/ELECTED OFFICE (DO/EO/US) CONCERNING A FILING UNDER 35 U.S.C. 371		**270031.401USPC** U S APPLICATION NO (If known, see37 CFR 1 5) **Unknown** **10/069676**
INTERNATIONAL APPLICATION NO. **PCT/JP00/05802**	INTERNATIONAL FILING DATE **28 August 2000 (28.02.00)**	PRIORITY DATE CLAIMED **27 August 1999 (27.08.99)**

TITLE OF INVENTION

IMAGE DATA DISTRIBUTION METHOD AND SYSTEM, IMAGE DATA AND RECORDING MEDIUM

APPLICANT(S) FOR DO/EO/US

SHINDO, Jiro

Applicant herewith submits to the United States Designated/Elected Office (DO/EO/US) the following items and other information:

1. ☒ This is a **FIRST** submission of items concerning a filing under 35 U.S.C. 371.
2. ☐ This is a **SECOND** or **SUBSEQUENT** submission of items concerning a filing under 35 U.S.C. 371.
3. ☒ This is an express request to begin national examination procedures (35 U.S.C. 371(f)). The submission must include items (5), (6), (9) and (21) indicated below.
4. ☒ The US has been elected by the expiration of 19 months from the priority date (Article 31).
5. ☒ A copy of the International Application as filed (35 U.S.C. 371(c)(2)).
   a. ☐ is attached hereto (required only if not communicated by the International Bureau).
   b. ☒ has been communicated by the International Bureau.
   c. ☐ is not required, as the application was filed in the United States Receiving Office (RO/US).
6. ☒ An English language translation of the International Application as filed (35 U.S.C. 371(c)(2)).
   a. ☒ is attached hereto
   b. ☐ has been previously submitted under 35 U.S.C. 154(d)(4).
7. ☒ Amendments to the claims of the International Application under PCT Article 19 (35 U.S.C. 371(c)(3)).
   a. ☐ are attached hereto (required only if not communicated by the International Bureau).
   b. ☐ have been communicated by the International Bureau.
   c. ☐ have not been made; however, the time limit for making such amendments has NOT expired.
   d. ☒ have not been made and will not be made.
8. ☐ A translation of the amendments to the claims under PCT Article 19 (35 U.S.C. 371(c)(3)).
9. ☐ An oath or declaration of the inventor(s) (35 U.S.C. 371(c)(4)).
10. ☒ A English language translation of the annexes to the International Preliminary Examination Report under PCT Article 36 (35 U.S.C. 371(c)(5)).

Items 11 to 20 below concern document(s) or information included:

11. ☐ An Information Disclosure Statement under 37 CFR 1.97 and 1.98.
12. ☐ An assignment document for recording. A separate cover sheet in compliance with 37 CFR 3.28 and 3.31 is included.
13. ☐ A FIRST preliminary amendment.
14. ☐ A SECOND or SUBSEQUENT preliminary amendment.
15. ☒ A substitute specification.
16. ☐ A change of power of attorney and/or address letter.
17. ☐ A computer-readable form of the sequence listing in accordance with PCT Rule 13ter.2 and 35 U.S.C. 1.821 – 1.825.
18. ☐ A second copy of the published international application under 35 U.S.C. 154(d)(4)
19. ☐ A second copy of the English language translation of the international application under 35 U.S.C. 154(d)(4).
20. ☐ Other items of information:

EXPRESS MAIL NO. EV064839849US

U.S. APPLICATION NO (If known, see 37 CFR 1.5)	INTERNATIONAL APPLICATION NO.	ATTORNEY'S DOCKET NUMBER
Unknown 10/069676	PCT/JP00/05802	270031.401USPC

21. ☒ The following fees are submitted:	CALCULATIONS PTO USE ONLY	
Basic National Fee (37 CFR 1.492(a)(1)-(5)):		
Neither international preliminary examination fee (37 CFR 1.482) nor international search fee (37 CFR 1.445(a)(2)) paid to USPTO and International Search Report not prepared by the EPO or JPO $1040.00		
International preliminary examination fee (37 CFR 1.482) not paid to USPTO but International Search Report prepared by the EPO or JPO $890.00		
International preliminary examination fee (37 CFR 1.482) not paid to USPTO but international search fee (37 CFR 1.445(a)(2)) paid to USPTO $740.00		
International preliminary examination fee (37 CFR 1.482) paid to USPTO but all claims did not satisfy provisions of PCT Article 33(1)-(4)..... $710.00		
International preliminary examination fee (37 CFR 1.482) paid to USPTO and all claims satisfied provisions of PCT Article 33(1)-(4) $100.00		
ENTER APPROPRIATE BASIC FEE AMOUNT =	$890.00	
Surcharge of $130.00 for furnishing the oath or declaration later than ☐ 20 ☒ 30 months from the earliest claimed priority date (37 CFR 1.492(e)).	$130.00	

Claims	Number Filed	Number Extra	Rate		
Total Claims	33 - 20 =	13	x $ 18.00	$234.00	
Independent Claims	6 - 3 =	3	x $ 84.00	$252.00	
Multiple dependent claim(s) (if applicable)			+ $280.00	$0.00	
TOTAL OF ABOVE CALCULATIONS =				$1,506.00	
☐ Applicant claims small entity status. See 37 CFR 1.27. The fees indicated above are reduced by 1/2.				$.00	
SUBTOTAL =				$1,506.00	
Processing fee of $130.00 for furnishing the English translation later than ☐ 20 ☐ 30 months from the earliest claimed priority date (37 CFR 1.492(f)). +				$0.00	
TOTAL NATIONAL FEE =				$1,506.00	
Fee for recording the enclosed assignment (37 CFR 1.21(h)). The assignment must be accompanied by an appropriate cover sheet (37 CFR 3.28, 3.31). $40.00 per property +				$0.00	
TOTAL FEES ENCLOSED =				**$1,506.00**	
				Amount to be refunded.	
				charged	

a. ☒ A check in the amount of $1,506.00 cover the above fees is enclosed.

b. ☐ Please charge my Deposit Account No. in the amount of $_ to cover the above fees. A duplicate copy of this sheet is enclosed.

c. ☒ The Commissioner is hereby authorized to charge any additional fees which may be required, or credit any overpayment to Deposit Account No. **19-1090**. A duplicate copy of this sheet is enclosed.

d. ☐ Fees are to be charged to a credit card. WARNING: Information on this form may become public. Credit card information should not be included on this form. Provide credit card information and authorization on PTO-2038.

NOTE: Where an appropriate time limit under 37 CFR 1.494 or 1.495 has not been met, a petition to revive (37 CFR 1.137(a) or (b)) must be filed and granted to restore the application to pending status.

SEND ALL CORRESPONDENCE TO:

David V. Carlson, Esq.
Seed Intellectual Property Law Group PLLC
701 5th Avenue, Suite 6300
Seattle, WA 98104-7092
United States of America
(206) 622-4900

SIGNATURE

David V. Carlson
NAME

31,153
REGISTRATION NUMBER

PATENT COOPERATION TREATY

Int'l Application No.	:	PCT/JP00/05802
Int'l Filing Date	:	28 August 2000
U.S. Application No.	:	Not yet known
Inventors	:	SHINDO, Jiro
Title	:	IMAGE DATA DISTRIBUTION METHOD AND SYSTEM, IMAGE DATA AND RECORDING MEDIUM
Docket No.	:	270031.401USPC
Date	:	21 February 2002

Box PCT
Assistant Commissioner for Patents
Washington, DC 20231-0001

PRELIMINARY AMENDMENT

Sir:

Please enter a Preliminary Amendment by replacing the application and claims presently on file as identified above with the enclosed substitute specification and claims prior to examination on the merits.

Respectfully submitted,

Seed Intellectual Property Law Group PLLC

David V. Carlson
Registration No. 31,153

DVC:km

701 Fifth Avenue, Suite 6300
Seattle, Washington 98104-7092
(206) 622-4900; Fax: (206) 682-6031

IMAGE DATA DISTRIBUTION METHOD AND SYSTEM, IMAGE DATA AND RECORDING MEDIUM

TECHNICAL FIELD

The present invention pertains to technology for network distribution of a digitized image; particularly, to an image data distribution method and a system therefore as well as image data to be utilized therein.

BACKGROUND OF THE INVENTION

In general, since digital image data distributed via a network, such as the Internet, can be easily duplicated without impairing the picture quality, such data should be protected against illegal use; for example, against redistribution and/or duplication by unauthorized individuals. Thus, Japanese Kokai Patent Application No. Hei 9[1997]-191394, for example, discloses a method referred to as an electronic watermark or digital watermarking, which has been developed in order to embed copyright and source information in the image data to be distributed.

However, this type of electronic watermarking, which merely adds the copyright source, has the problem that even when illegal use occurs, the distribution route of the data, that is, when, to which clients, and under what conditions was the data distributed, could not be specified. Thus, for example, Japanese Kokai Patent Application No. 2000-50047 discloses a data distribution method in which information for designating the distribution destination is embedded in the image data. However, even with this data distribution method, because no information on which user is responsible is contained, the redistribution route of data is unlikely to be specified accurately.

Thus, the purpose of the present invention is to present an image data distribution method and a system therefor with which actual use of distributed image data by users can be found accurately, the redistribution route of the data can be specified easily in the event of an illegal use, and illegal use of the image data can be prevented or effectively curtailed.

SUMMARY OF THE INVENTION

The present invention concerns an image data distribution method that contains a step in which image data distributed from the server side is unarchived to a memory on the client side, and user security data is then added to the unarchived image data in order to prevent illegal use of image data resulting from the distribution of image data from the server side to the client side via a network.

Accordingly, security data, that is, user or client identification data for the prevention of illegal use, can be added to the image data by the client who received the distributed image data, so that if the image data is used illegally, its redistribution route can be easily traced. Thus, an effective psychological restraint against the illegal use of image data can be achieved.

In a particular application example, a process in which the user security data is transmitted from the client side to the server side and a step in which said security data is stored in a storage device on the server side are included wherein security data added to given image data and the security data stored on the server side can be cross-referenced in the event of illegal use of the image, so that the redistribution route of the image data can be more accurately traced.

Preferably, the security data may be added to image data in the form of an electronic watermark.

More preferably, the security data can be added to the image data by selecting several pixels at non-adjacent positions locations among the pixels for the image data unarchived to a memory and by increasing or decreasing the luminance level of the pixels selected.

In one possible embodiment, the present invention concerns an image data distribution method that it includes a step in which an instruction is given so that the client can gain access to a security controller which performs authorization for image data distribution in response to a request made by the client, and a step in which an electronic key for unarchiving the image data is transmitted from the security controller to the client side in response to the authorization request for image data distribution from the client side on the server side in order to prevent illegal use of

image data resulting from the distribution of image data from the server side to client side via a network.

When distribution destinations are verified in advance in this manner, the image data can be prevented from being distributed to unauthorized users or clients.

In a particular application example, a step for storing the communication status on the client side is provided. Accordingly, said distribution destination can be easily identified on the server side after the distribution of image data, so that in the event of illegal use, its redistribution route can be easily traced.

In another application example, it is desirable that a security controller be provided separately from the server used for image data distribution, and the client side is instructed to gain access to the security controller using a IP address given to it.

In another application example of the present invention, a storage medium containing software for the execution of said image data distribution method is presented on the client side or the server side.

In yet another possible embodiment of the present invention, the image data distribution method includes a method for distributing image data from a server to clients and comprises a step in which an instruction for the client side to gain access to a security controller is given from the server side in response to a request for image data by the client, a step in which the client gains access to the security controller in order to be authorized for image data distribution, a step in which image data corresponding to the request is transmitted from the server side to the client side, a step in which an image key for opening the image data is transmitted from the server side to the client side, a step in which the image data is unarchived using the image key on the client side, and user security data is added to said image data, and a step in which the image data to which the security data has been added is output.

When so configured, because distribution destinations can be verified in advance in order to prevent image data from being distributed to unauthorized users or clients, and a client who actually received the image data can add security data, that is, user or client identification data for the prevention of illegal use, to the image data, the redistribution route in the event of illegal use of the image data can be easily traced.

Therefore, not only can the illegal use of image data be effectively prevented, but also there results a strong psychological restraint against the illegal use of image data.

In another application example, because a step in which the security data is transmitted to the server side and a step in which said security data is stored by the server are further provided, in the case of illegal use of image data, the security data that has been added to the image data and the security data stored by the server can be cross-referenced in order to trace and specify the redistribution route of the image data more accurately.

In another application example, because the server is further provided with a step in which communication status with the client is stored in a log file, a client or user culpable of illegal use can be specified more accurately and easily.

In addition, in another application example, it is desirable that a security controller be provided separately from the server used for image data distribution, and access to the security controller is instructed by giving an IP address to the client side.

In another application example, image data transmitted from the server side is compressed, so that the security data can be added after said image data is unarchived on the client side.

In addition, it is desirable that the security data be added to the image data in the form of an electronic watermark.

In a specific application example, the security data can be added to the image data by selecting several pixels at non-adjacent positions locations among the pixels for the image data unarchived using the image key and by increasing or decreasing the luminance level of the selected pixels.

The date and time of the distribution of the image data, user ID, and the serial number of the client storage device storing the image data or the IP address of the client may be included in the security data. When they are utilized, the redistribution route after the distribution of the image data can be easily traced.

The present invention also provides an image data distribution system that is equipped with an image file server having an image file database containing image files, a security control server having a user database containing registration data on respective users and an image key database containing image keys for unarchiving

respective image files to clients, and a network for connecting the image file server, the security control server, and the clients; wherein, the image file server has a function of instructing a client to gain access to the security control server in response to a request from said client for image data and a function of transmitting the image data requested to the client, the client has a function of gaining access to the security control server to request for user authorization in order to obtain the image data, the security control server has functions of verifying via the user database, the user in response to the client's request for authorization and of then transmitting the image key to the requested image data from the image key database, and the client is further provided with functions for unarchiving the image data received using the image key and for adding user security data to said image data.

When so configured, distribution destinations can be authorized in advance in order to prevent image data from being distributed to unauthorized users or clients, and the redistribution route of image data can be specified easily, since security data, that is, user or client identification data, is added to the image data by the client who received the image data, so that an image data distribution method with which illegal use of image data can be prevented and psychologically discouraged more reliably than ever can be realized.

In a particular application example, because the client has also the function of transmitting the security data to the security control server, and the security control server also has the function of storing the security data, the security data in the image data and the one stored in the security control server can be cross-referenced at a later time.

In another application example, because the security control server has a log file to store the communication status with a client, the image data distribution status can be ascertained more accurately.

It is desirable that the image file server give the instruction for gaining access to the security control server through the provision of the IP address.

In a particular application example, image data transmitted from the image file server is compressed, so that the client unarchives the image data received before adding the security data.

It is desirable that the client add the security data to the image data in the form of an electronic watermark.

In addition, it is convenient if the security data contain the date and time of the distribution of the image data, user ID, and the serial number of the client's storage device storing the image data or the IP address of the client when specifying the redistribution route of the image data.

Furthermore, the present invention also provides image data with embedded user information by increasing or decreasing the luminance levels of several selected pixels placed at discrete locations on a map of pixel data represented by dots.

BRIEF DESCRIPTION OF THE DRAWINGS

Figure 1 is a diagram showing the outlined configuration of a preferred application example of the image data distribution system in accordance with the present invention.

Figure 2 is a flowchart showing the process of image data distribution in the image data distribution system in Figure 1.

DETAILED DESCRIPTION OF THE INVENTION

Figure 1 shows the outline of a system configuration on the Internet as a preferred application example of the image distribution system in accordance with the present invention. The image distribution system in the present application example is configured with multiple clients (2) connectable via a network environment, such as the Internet (1), an image filer server (3), and a security control server (4). The client (2) is a computer provided with functions for transmitting a request specifying a desired image to the image file server (3) using WWW browser on the Internet (1) in order to receive digital image data from said server and for regenerating the image.

The image file server (3) is made of a computer for transmitting image data in response to the request from the client (2) on the Internet and provided with a file database (5) containing image files and a log file (6) for storing communication status with the client (2). Furthermore, the image file server (3) has the function of transmitting an IP address for the security control server (4) in response to the request

for image data from the client (2) in order to instruct the client (2) to gain access to the security control server and the function of transmitting the requested image data from the image file database (5) to the client.

In the present application example, compressed hierarchized image files having a data structure in which digitized image data is hierarchized once according to the significance of the information the respective pixels have (for example, luminance level or changes in luminance level). The pixels are then restructured and for another example, stored in the image file database (5). These hierarchized image files can be generated using, for example, the image compression method described in the specifications of International Patent Application Nos. PCT/JP00/04472, PCT/JP/05801 and PCT/JP00/05802, all by the inventor of the present application, and all of which are incorporated herein by reference. Said hierarchized image files comprise information on the positions and the luminance levels of respective pixels. Because the images differ in terms of quality, that is, resolution, depending on their ranking and size, the client can specify the image quality when requesting image data.

The security control server (4) has a user database (7) containing the contents of the registrations of users who are allowed to utilize the image files in the image file database (5), an image key database (8) containing the necessary image keys for unarchiving the image files, and a log file (9) for storing communication statuses with clients (2). Respective users and their identification data are classified into several groups and registered in the user database (7) of the present application example. Each group is granted certain rights, so that they select the corresponding quality, that is, resolution, and size.

The client (2) can gain access to the security control server using the IP address for the security control server (4) received from the image file server (3) in order to request for authorization to acquire the image data. The security control server (4) verifies the user through database (7) in response to said authorization request and transmits an image key peculiar to the image data requested from the image key database (8).

The client (2) is also able to unarchive the image data received from the image file server (3) into the memory using the image key and to add user security data

to said image data. Said security data contains identification data on the client or user, such as the date and time of the distribution of the image data, user ID, serial number of the storage device, for example, a hard disk drive, to which the image data was downloaded, IP address of the client (2), which are useful for tracing the redistribution route in the event of illegal use.

Next, a preferred application example of the image distribution method in accordance with the present invention will be explained using Figure 2. First, the client (2) activates a general-purpose or WWW-dedicated browser in order to get connected to the image file server (3) via the Internet. Once the client (2) transmits a request specifying the name and the quality of the desired image file (step S1), the image file server (3) returns an IP address for the security control server (4) (step S2). The client (2) gains access to the security control server (4) using said IP address in order to request for authorization to acquire the image data (step S3). User ID, client's IP address, and serial number of the hard disk drive as data peculiar to the client are utilized for said authorization.

The security control server (4) verifies registered data, such as user ID, in reference to the user database (7) before granting authorization (step S4). Then, an image key peculiar to the image data requested is obtained from the image key database (8) and transmitted to the client (2) (step S5), and the status of this communication is stored in the log file at the same time (9) (step S6). On the other hand, the image filer server (3) obtains the image data requested from the image file database (5) and transmits it to the client (2) (step S7). Similarly, the image file server (3) also stores the communication status with the client (2) in the log file (6).

The client (2) opens and decompresses the image data received from the image file server (3) using the image key received from the security control server (4) and unarchives it to memory as a pixel data map of the respective pixels constituting the image (step S8). Then, the security data is encoded and added to the unarchived image data (step S9). In general, the addition of security data is achieved using a so-called electronic watermark or an electronic window. In the present application example, an electronic watermark can be inserted by selecting several pixels placed at non-adjacent discontinuous positions locations among the pixels for the unarchived image data and

increasing or decreasing the luminance levels of the pixels. The positions of the pixels can be selected in advance, and they can be also changed depending on the contents of the image.

The image data to which the security data has been added in said manner is output (step S10) and can be utilized in a variety of ways; for example, displayed directly on the client's display, stored in a storage device, such as a hard disk drive, or other storage media; or transmitted on-line to another apparatus. At the same time, the client (2) transmits the security data to the security control server (4) (step S11), and the security control server (4) stores it in the log file (9) (step S12).

As a result, because a record on the distribution of the image data is kept in the security control server (4), in the event of subsequent illegal use of the image data, its redistribution route can be easily specified by cross-referencing the security data embedded in the image data. In addition, in the present application example, because the image file server (3) and the security control server (4) are provided separately, security data transmitted from clients can be managed once the address of the security control server (4) is preset on the network even when the image file server (3) is set to an arbitrary address as needed, that is, when the image file database (5) is set to an arbitrary address.

In another application example of the present invention, the image file server (3) and the security control server (4) can be integrated in order to use a single server for the configuration. In this case, access to the security control server (4) and use of the image key can be omitted. That is, the client (2) first requests authorization from the server for image distribution; and after the server has granted authorization in reference to the user database (7) in response to said request, the client (2) requests distribution of the desired image in order to have the image transmitted. Needless to say, in this case, too, after the client has opened the image data and unarchived it into the memory, security data is added to the image data in the same manner as that in the application example and transmitted to the server, and the server stores it into the log file.

Moreover, in yet another application example, the IP address for the security control server (4) can be added to the image data distributed from the image file

server (3) in advance. In this case, upon receiving an image data distribution request from the client (2), the image file server (3) transmits the image data requested. The client (2) reads the IP address from the image data received and gains access to the security control server (4) in order to request authorization. Once the security control server (4) completes authorization and transmits the image key, the client (2) is able to open the image data using said image key.

A number of examples of the present invention have been explained in detail herein. As is clear to an expert in the field, the present invention can be implemented with various kinds of changes and modifications to the example herein within the scope of the invention. For example, in one embodiment, the present invention can also be applied to a network other than the Internet and the steps carried out in the same manner as described herein.

From the foregoing it will be appreciated that, although specific embodiments of the invention have been described herein for purposes of illustration, various modifications may be made without deviating from the spirit and scope of the invention. Accordingly, the invention is not limited except as by the appended claims.

Claims

1. A method for delivering image data, characterized by including a process that develops image data delivered from a server side on a memory at a client side and adds security data of a user to the image data developed in order to prevent illegal use of the image data in the delivery of the image data to the above-mentioned client side via a network from the above-mentioned server side.

2. The method for delivering image data of Claim 1, characterized by further including a process that transmits the security data of the above-mentioned user to the above-mentioned server side from the above-mentioned client side and a process that stores the above-mentioned security data in a storage device of the above-mentioned server side.

3. The method for delivering image data of Claim 1 or 2, characterized by adding the above-mentioned security data as an electronic window to the above-mentioned image data.

4. The method for delivering image data of any of Claims 1-3, characterized by the fact that the above-mentioned security data are added to the above-mentioned image data by selecting several picture elements existing at noncontinuous positions among respective picture elements of the above-mentioned image data developed on the memory and increasing or decreasing the luminance of the above-mentioned picture elements selected.

5. A method for delivering image data, characterized by including a process that instructs a client side to access a security controller for certifying image data delivery in response to a request from the above-mentioned client at a server side in order to prevent illegal use of image data in the delivery of the image data to the above-mentioned client side via a network from the above-mentioned server side; a process that delivers an electronic key for opening the image data to the above-mentioned client side from the above-mentioned security controller in response to the certification request of the image data delivery from the above-mentioned client side.

6. (Deletion)

7. (Deletion)

8. (Deletion)

9. A method for delivering image data, characterized the fact that in a method for delivering image data to a client from a server, it includes a process that instructs the above-mentioned client side to access a security controller from the server side in response to the request of the image data from the client side, a process that accesses the above-mentioned security controller from the above-mentioned client side and demands the certification of an image data delivery, a process that transmits the image data corresponding to the above-mentioned request to the above-mentioned client side from the above-mentioned server side, a process that transmits an image key for opening the above-mentioned image data to the above-mentioned client side from the above-mentioned server side, a process that opens the

above-mentioned image data by using the above-mentioned image key at the above-mentioned client side and adds security data of the user or client to said image data, and a process that outputs the image data to which the above-mentioned security data are added.

10. (Deletion)

11. (Deletion)

12. (Deletion)

13. (Deletion)

14. (Deletion)

15. (Deletion)

16. (Deletion)

17. An image data delivery system, characterized by the fact that it is equipped with an image file server that has an image file database in which image files are stored, a security control server that has a user database in which registered data of each user are stored and an image key database in which image keys for opening the above-mentioned each image file are stored, clients and a network that connects the above-mentioned image file server, the above-mentioned security control server, and the above-mentioned clients; and it has a function that instructs an above-mentioned client to access the above-mentioned security control server in response to the request of image data from the above-mentioned client by the above-mentioned image file server, a function that transmits the image data requested to the above-mentioned client, a function that accesses the above-mentioned security control server by the above-mentioned client and requests certification of the above-mentioned image data acquisition of the user, a function that responds to the request of certification from the above-mentioned client by the above-mentioned security control server, confirms the above-mentioned user database, gives the certification to the above-mentioned user, and transmits the image keys of the above-mentioned requested image data from the above-mentioned image database, and a function that opens the above-mentioned received image data by the above-mentioned client using the image keys and adds security data of the above-mentioned user to the above-mentioned image data.

18. (Deletion)

19. (Deletion)

20. (Deletion)

21. (Deletion)

22. (Deletion)

23. (Deletion)

24. Image data, characterized by the fact that information of a user is embedded by increasing or decreasing the luminance of several selected picture elements which are constituted by a map of picture element data of individual dots with positions that are not continuous.

25. (Addition) The method for delivering image data of Claim 5, characterized by the fact that the above-mentioned image data have image files of varying image quality; and the request from the above-mentioned client includes a designation of image quality.

26. (Addition) The method for delivering image data of Claim 25, characterized by the fact that the above-mentioned image data have image files with a data structure which is made hierarchical by the image quality.

27. (Addition) The method for delivering image data of Claim 25 or 26, characterized by the fact that the above-mentioned image quality is the resolution or size of the images.

28. (Addition) The method for delivering image data of any of Claims 5 and 25-27, characterized by further including a process that saves a communication condition with the above-mentioned client side.

29. (Addition) The method for delivering image data of any of Claims 5 and 25-28, characterized by the fact that access to the above-mentioned security controller is instructed by giving an IP address of the above-mentioned security controller.

30. (Addition) A recording medium for storing software to implement the method for delivering image data of any of Claims 1-3, 5, and 25-29.

31. (Addition) The method for delivering image data of Claim 9, characterized by the fact that the above-mentioned image data have image files of varying image quality; and the request from the above-mentioned client includes a designation of image quality.

32. (Addition) The method for delivering image data of Claim 31, characterized by the fact that the above-mentioned image data have image files with a data structure which is made hierarchical by the image quality.

33. (Addition) The method for delivering image data of Claim 31 or 32, characterized by the fact that the above-mentioned image quality is the resolution or size of the images.

34. (Addition) The method for delivering image data of any of Claims 9 and 31-33, characterized by further including a process that transmits the above-mentioned security data to the above-mentioned server side and a process that saves said security data at the above-mentioned server side.

35. (Addition) The method for delivering image data of any of Claims 9 and 31-34, characterized by further including a process that saves a communication conditions with the above-mentioned client side in a log file at the above-mentioned server side.

36. (Addition) The method for delivering image data of any of Claims 9 and 31-35, characterized by the fact that access to the above-mentioned security controller is instructed by giving an IP address of the above-mentioned security controller.

37. (Addition) The method for delivering image data of any of Claims 9 and 31-36, characterized by the fact that the above-mentioned image data being transmitted from the above-mentioned server side are compressed; and after said image data are expanded at the above-mentioned client side, the above-mentioned security data are added.

38. (Addition) The method for delivering image data of any of Claims 9 and 31-37, characterized by the fact that the above-mentioned security data are added as an electronic window to the above-mentioned image data.

39. (Addition) The method for delivering image data of any of Claims 9 and 31-38, characterized by the fact that the above-mentioned security data are added to the above-mentioned image data by selecting several picture elements existing at discontinuous positions among respective picture elements of the above-mentioned image data, opened by using the above-mentioned image key, and increasing or decreasing the luminance of the above-mentioned picture elements selected.

40. (Addition) The method for delivering image data of any of Claims 9 and 31-39, characterized by the fact that the delivery date of the above-mentioned image data, user ID, serial number of the storage device of the above-mentioned client in which the above-mentioned image data are stored, or IP address of the above-mentioned client are included in the above-mentioned security data.

41. (Addition) The image data delivery system of Claim 17, characterized by the fact that the above-mentioned image data have image files of varying image quality; and the request from the above-mentioned client includes a designation of image quality.

42. (Addition) The image data delivery system of Claim 41, characterized by the fact that the above-mentioned image data have image files with a data structure which is made hierarchical by the image quality.

43. (Addition) The image data delivery system of Claim 41 or 42, characterized by the fact that the above-mentioned image quality is the resolution or size of the images.

44. (Addition) The image data delivery system of any of Claims 17 and 41-43, characterized by further having a function that transmits the above-mentioned security data to the above-mentioned security control server by the above-mentioned client and a function that saves the above-mentioned security data by the above-mentioned security control server.

45. (Addition) The image data delivery system of any of Claims 17 and 41-44, characterized by the fact that the above-mentioned security control server has a log file for saving a communication conditions with the above-mentioned client.

46. (Addition) The image data delivery system of any of Claims 17 and 41-45, characterized by the fact that the above-mentioned image file server instructs an access to the security control server by giving an IP address of the above-mentioned security control server.

47. (Addition) The image data delivery system of any of Claims 17 and 41-46, characterized by the fact that the above-mentioned image data being transmitted from the above-mentioned file server are compressed; and after said image data received are expanded by the above-mentioned client, the above-mentioned security data are added.

48. (Addition) The image data delivery system of any of Claims 17 and 41-47, characterized by having a function that adds the above-mentioned security data as an electronic window to the above-mentioned image data by the above-mentioned client.

49. (Addition) The image data delivery system of any of Claims 17 and 41-48, characterized by the fact that delivery date of the above-mentioned image data, user ID, serial number of the storage device of the above-mentioned client in which the above-mentioned image data are stored, or IP address of the above-mentioned client are included in the above-mentioned security data.

ABSTRACT OF THE DISCLOSURE

An image distribution system is configured with multiple client connectable via a network environment, such as Internet, an image file server having image file database containing image files and log file, user database, and security control server having image key database and log file. Image data from the image file server can be opened once the client who made the image data request gains access to the security control server using an IP address obtained from the image file server, is granted authorization, and obtains an image key. The client encodes security data, such as the date and time of the distribution of the image data, user ID, serial number of hard disk drive, and client's IP address, in order to embed it in the image data unarchived into its memory in the form of an electronic watermark and transmits the security data to the security control server in order to store it in the log file at the same time.

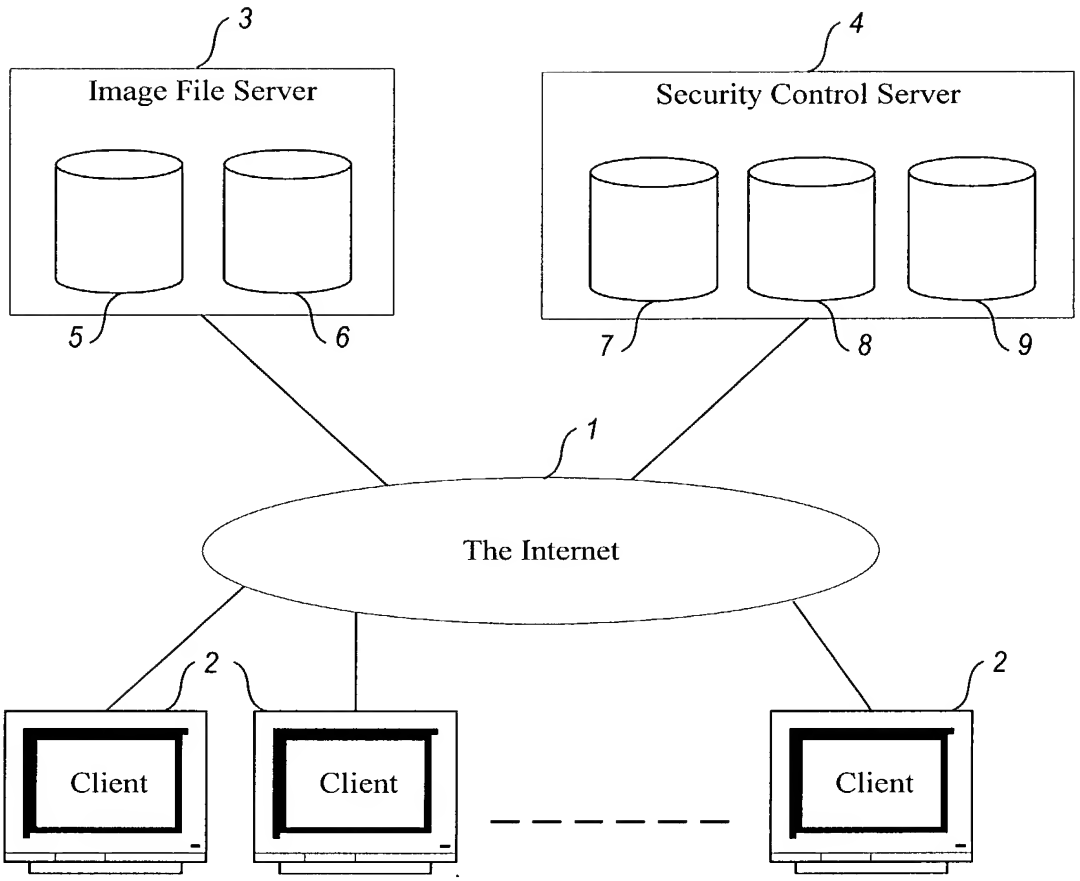
3
Image File Server
4
Security Control Server
5
6
7
8
9
1
The Internet
2
2
Client
Client
Client

Fig. 1

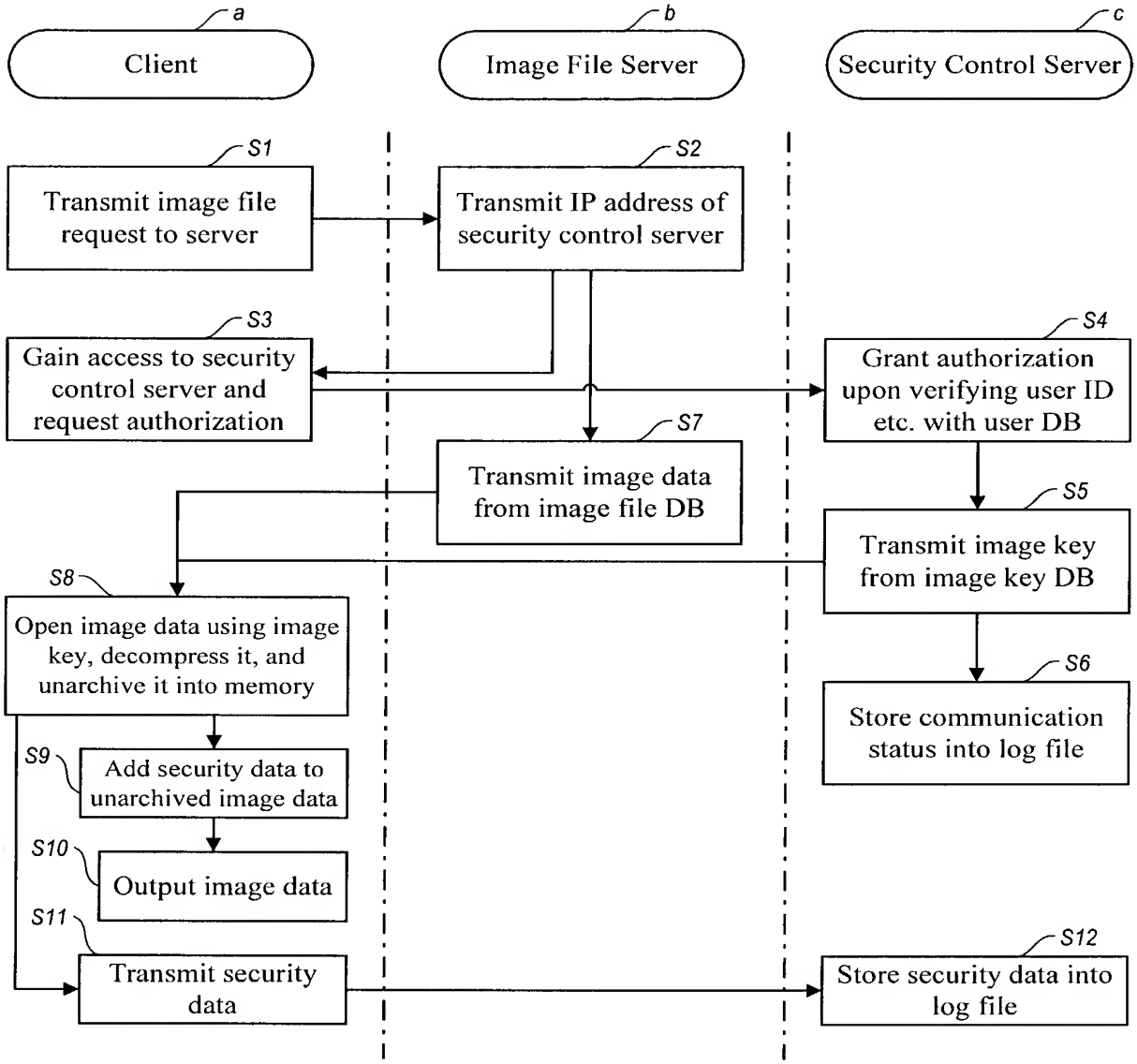
a
Client
b
Image File Server
c
Security Control Server
S1
Transmit image file request to server
S2
Transmit IP address of security control server
S3
Gain access to security control server and request authorization
S4
Grant authorization upon verifying user ID etc. with user DB
S7
Transmit image data from image file DB
S5
Transmit image key from image key DB
S8
Open image data using image key, decompress it, and unarchive it into memory
S6
Store communication status into log file
S9
Add security data to unarchived image data
S10
Output image data
S11
Transmit security data
S12
Store security data into log file

Fig. 2

Please type a plus sign (+) inside this box → [+]

Express Mail No.: EV170133837US

EXPRESS MAIL NO. EV064839849US

PTO/SB/81 (10-00)
Approved for use through 10/31/2002. OMB 0651-0035
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number

ELECTION AND POWER OF ATTORNEY OR AUTHORIZATION OF AGENT

Application Number	NA
Filing Date	NA
First Named Inventor	Jiro Shindo
Group Art Unit	Not yet known
Examiner Name	Not yet known
Attorney Docket Number	270031.401USPC

I hereby appoint:

[X] Practitioners at Seed IP Law Group PLLC

OR

[ ] Practitioner(s) named below:

00500
PATENT TRADEMARK OFFICE

Name	Registration Number

as my/our attorney(s) or agent(s) to prosecute the application identified above, and to transact all business in the Patent and Trademark Office connected therewith.

Please change the correspondence address for the above-identified application to:

[ ] The above-mentioned Customer Number.

OR

[ ] Firm *or* Individual Name					
Address					
Address					
City		State		ZIP	
Country					
Telephone		Fax			

I am the:

[ ] Applicant/Inventor.

[X] Assignee of record of the entire interest. See 37 CFR 3.71.

Statement under 37 CFR 3.73(b) is enclosed. (Form PTO/SB/96).

[X] As assignee of record of the entire interest hereby elect, under 37 C.F.R. § 3.71, to prosecute the application to the exclusion of the inventor

SIGNATURE of Applicant or Assignee of Record

Name	Jiro Shindo
Signature	
Date	10/06/02

NOTE: Signatures of all the inventors or assignees of record of the entire interest or their representative(s) are required. Submit multiple forms if more than one signature is required, see below*

[X] *Total of 4 forms are submitted.

Burden Hour Statement: This form is estimated to take 3 minutes to complete. Time will vary depending upon the needs of the individual case. Any comments on the amount of time you are required to complete this form should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, Washington, DC 20231. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Assistant Commissioner for Patents, Washington, DC 20231

Express Mail No.: EV170133837US

EXPRESS MAIL NO. EV064839849US

Please type a plus sign (+) inside this box [+]

PTO/SB/01 (10-01) (modified)

DECLARATION FOR UTILITY OR DESIGN PATENT APPLICATION (37 CFR 1.63)		
	Attorney Docket No.	270031.401USPC
	First Named Inventor	Jiro Shindo
	COMPLETE IF KNOWN	
	Application Number	NA
	Filing Date	NA
[X] Declaration Submitted with Initial Filing [ ] Declaration Submitted after Initial Filing	Group Art Unit	Not yet known
	Examiner's Name	Not yet known

As the below named inventor(s), I/we hereby declare that:

My residence, post office address, and citizenship are as stated below next to my name.

I/we believe that I/we am/are the original and first inventor(s) of the subject matter which is claimed and for which a patent is sought on the invention entitled:

IMAGE DISTRIBUTING METHOD AND SYSTEM, IMAGE DATA, AND RECORDED MEDIUM

(Title of Invention)

the specification of which was filed on (MM/DD/YYYY) **August 28, 2000** the specification of which is attached hereto [ ]

as United States Application Number or PCT International Application Number **PCT/JP00/05802** Express Mail No.

and was amended on (MM/DD/YYYY) *(if applicable)*

I/we have reviewed and understand the contents of the above identified specification, including the claims, as amended by any amendment specifically referred to above.

In addition, I/we acknowledge the duty to disclose to the United States Patent and Trademark Office all information known to me/us to be material to patentability as defined in 37 CFR 1.56, including material information which became available between the filing date of the prior application and the National or PCT International filing date of the continuation-in-part application, if applicable.

I/we hereby claim foreign priority benefits under 35 U.S.C. 119(a)-(d) or (f), or 365(b) of any foreign application(s) for patent or inventor's certificate, or 365(a) of any PCT international application which designated at least one country other than the United States of America, listed below and have also identified below, by checking the box, any foreign application for patent or inventor's certificate, or of any PCT international application having a filing date before that of the application on which priority is claimed.

Prior Foreign Application Number(s)	Country	Foreign Filing Date (MM/DD/YYYY)	Priority Claimed	Certified Copy Attached? YES	NO
11/283295	JP	August 27, 1999	Y		X
T/JP00/05802	WO	August 28, 2000	Y		X

Additional foreign application numbers are not listed on a supplemental priority data sheet PTO/SB/02B attached hereto.

I/we hereby claim the benefit under 35 U.S.C. 119(e) of any United States provisional application(s) listed below.

Application No.	Filing Date (MM/DD/YYYY)	Application No.	Filing Date (MM/DD/YY)

Additional provisional application numbers are not listed on a supplemental priority data sheet PTO/SB/02B attached hereto.

Direct all communications to Customer Number **00500**

Name	David V. Carlson	of SEED INTELLECTUAL PROPERTY LAW GROUP PLLC					
Address	701 Fifth Avenue, Suite 6300						
City	Seattle		*State*	WA	*Zip*	98104-7092	
Country	U.S.A.	*Telephone*	(206) 622-4900	*Fax*	(206) 682-6031		

I/we hereby declare that all statements made herein of my/our own knowledge are true and that all statements made herein on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like are punishable by fine or imprisonment, or both, under 18 U.S.C. 1001 and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

Sole or First Inventor:	Jiro Shindo					
Given Name (first and middle [if any])			Family Name or Surname			
Jiro			SHINDO			
Inventor's Signature			Date	10/06/02		
Residence: City	Kyoto	State		Country	JP	Citizenship	JP
Post Office Address	c/o K.K. Digital Publishing Japan, 196-1 Kamigamohonzan, Kita-ku, Kyoto-shi					
City	Kyoto 603-8047	State	JPX	Country	JP	

Additional Inventor:						
Given Name (first and middle [if any])			Family Name or Surname			
Inventor's Signature			Date			
Residence: City		State		Country		Citizenship	
Post Office Address						
City		State		Country		

Additional Inventor:						
Given Name (first and middle [if any])			Family Name or Surname			
Inventor's Signature			Date			
Residence: City		State		Country		Citizenship	
Post Office Address						
City		State		Country		

Additional Inventor:						
Given Name (first and middle [if any])			Family Name or Surname			
Inventor's Signature			Date			
Residence: City		State		Country		Citizenship	
Post Office Address						
City		State		Country		

D:\NrPortbl\iManage\KRISTINA\251744_1 DOC

SCANNED,# 12

United States Patent & Trademark Office

Office of Initial Patent Examination -- Scanning Division

Application deficiencies found during scanning:

☑ Page(s) 1 of Claim was ~~were~~ not present for scanning.
(Document title)

☐ Page(s)_____ of _____ were not present for scanning.
(Document title)

☐ ***Scanned copy is best available.***

there are specification page #out of order
page numbers out of order